Brief Announcement: Vehicle to Vehicle Authentication*

Shlomi Dolev[1], Łukasz Krzywiecki[2], Nisha Panwar[1], and Michael Segal[3]

[1] Department of Computer Science, Ben-Gurion University of the Negev, Israel. {dolev, panwar}@cs.bgu.ac.il.

[2] Institute of Mathematics and Computer Science, Wrocław University of Technology, Poland. lukasz.krzywiecki@pwr.wroc.pl.

[3] Department of Communication Systems Engineering, Ben-Gurion University of the Negev, Israel. segal@cse.bgu.ac.il.

Vehicle Authentication. In recent future, vehicles will establish a spontaneous connection over a wireless radio channel, coordinating actions and information. Vehicles will exchange warning messages over the wireless radio channel through Dedicated Short Range Communication (IEEE 1609) over the Wireless Access in Vehicular Environment (802.11p). Unfortunately, the wireless communication among vehicles is vulnerable to security threats that may lead to very serious safety hazards. Therefore, the warning messages being exchanged must incorporate an authentic factor such that recipient is willing to verify and accept the message in a timely manner.

Our Contribution. (*i*) Coupling fixed and non-fixed vehicle attributes with the public key, (*ii*) Optical out-of-band communication channel, (*iii*) Adaptation with existing authentication protocols, (*iv*) Verification.

Previous Work. Vehicles utilize wireless communication standard, i.e., IEEE 802.11p Wireless Access in Vehicular Environment (WAVE) based on IEEE 1609 Dedicated Short Range Communication (DSRC). Raya and Haubaux proposed a Public Key Infrastructure (PKI) based vehicle security scheme, however, an active adversary may launch an impersonation attack. Moreover, roadside infrastructure is required to provide the most updated Certificate Revocation List (CRL). Our scheme removes the active participation of roadside units as well as the regional authorities.

Problem Statement. Every vehicles public key is signed by the authorities and can be verified by the receiver, still, an impersonation attack among the moving vehicles is possible. Accordingly, the scenario starts when a vehicle v_1 tries to securely communicate with v_2 and requests for the public key of v_2.

* **This is a version that appeared as a brief announcement in 17th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS, 2015).** Partially supported by the Rita Altura Trust Chair in Computer Sciences, Lynne and William Frankel Center for Computer Sciences, Israel Science Foundation (grant 428/11), the Israeli Internet Association, and the Ministry of Science and Technology, Infrastructure Research in the Field of Advanced Computing and Cyber Security. Partially supported by fundings from Polish National Science Center (decision number DEC-2013/09/B/ST6/02251).

Vehicle v_3 pretends to be v_2 and answers v_1 with v_3 public key instead of v_2. Then v_3 concurrently asks v_2 for its public key. Vehicle v_1 is fooled to establish a private key with v_3 instead of v_2, and v_2 is fooled to establish a private key with v_3 instead of v_1. Vehicle v_3 conveys messages from v_1 to v_2 and back decrypting and re-encrypting with the appropriate established keys. In this way, v_3 can find the appropriate moment to change information and cause hazardous actions to v_1 and v_2.

System Model. (*i*) Light Amplification by Stimulated Emission of Radiation (LASER), (*ii*) LIght Detection And Ranging (LIDAR), (*iii*) Autocollimator, (*iv*) Physically Unclonable Function(PUF).

Proposed Scheme. The proposed approaches for the vehicle to vehicle authentication are summarized as below:
Basic Scheme [3] We propose to certify both the public key and out-of-band sense-able static attributes to enable mutual authentication of the communicating vehicles. Vehicle owners are bound to preprocess a certificate (periodically, possibly during the annual inspection procedure) that signs monolithically both a public key and a list of fixed unchangeable attributes (e.g., license number, brand and color) of the vehicle (extending ISO 3779 and 3780 standards). With such a scheme the vehicle can verify (say by using a camera) that the public key belongs to the specific vehicle to which the connection should be established (rather than a public key of a standing by adversary).
Intermediate Scheme [1] We consider the case of multiple malicious vehicles with identical visual static attributes. Apparently, dynamic attributes (e.g., location and direction) can uniquely define a vehicle and can be utilized to resolve the true identity of vehicles. However, unlike static attributes, dynamic attributes cannot be signed by a trusted authority beforehand. We propose an approach to verify the coupling between non-certified dynamic attributes and certified static attributes via an auxiliary laser communication channel.
Sophisticated Scheme [2] At last, we propose to use, the optical Physically Unclonable Function (PUF) to ensure that response from the receiving vehicle is spontaneous, rather than an answer forwarded from another vehicle. Vehicles utilize an out-of-band optical communication channel in order to exchange the PUF stimulated optical challenge and corresponding response from the sender and receiver, respectively.

Claims. We provide an extended proof of the proposed scheme using Spi calculus and BAN Logic, respectively. Our proposed approach adapts the security construction of the conventional Transport Layer Security (TLS) protocol and satisfy two crucial security properties, i.e., (*i*) Authentication: No active or passive adversary would be able to intercept the communication between sender and receiver and (*ii*) Secrecy: No active or passive adversary would be able to reveal neither the secret session messages nor the secret key.

References

1. S. Dolev, Ł. Krzywiecki, N. Panwar, and M. Segal. Dynamic attribute based vehicle authentication. In *IEEE 13th International Symposium on Network Computing and Applications (NCA)*, pages 1–8, 2014.
2. S. Dolev, Ł. Krzywiecki, N. Panwar, and M. Segal. Optical puf for vehicles non-forwardable authentication. Technical Report 15-02, Department of Computer Science, Ben-Gurion University of the Negev, 2015. Also appears as a Brief Announcement in IEEE NCA 2015.
3. S. Dolev, Ł. Krzywiecki, N. Panwar, and M. Segal. Vehicle authentication via monolithically certified public key and attributes. *Wireless Networks*, pages 1–18, 2015.